



Quarles & Brady LLP
Attorneys at Law
411 East Wisconsin Avenue
Suite 2400
Milwaukee, WI 53202-4428
414-277-5000
Fax 414-271-3552
quarles.com

Writer's Direct Dial: 414-277-5423
E-Mail: Meghan.OConnor@quarles.com

January 6, 2025

VIA EMAIL TO IDTHEFT@OAG.STATE.MD.US

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Dear Sir or Madam:

Pursuant to Md. Code Ann. Comm. Law 14-3504, this is to notify you about a security incident the Green Bay Packers, Inc. ("GBP") recently experienced and the steps they have taken in response.

On October 23, 2024, GBP was alerted to the presence of malicious code inserted on the Pro Shop website by a third party threat actor. Immediately upon learning this, GBP temporarily disabled all payment and checkout capabilities on the Pro Shop website and began an investigation. GBP engaged outside cybersecurity experts to assist with this investigation and determine what, if any, customer information may have been affected. GBP also immediately required the vendor that hosts and manages the Pro Shop website to remove the malicious code from the checkout page, refresh its passwords, and confirm there were no remaining vulnerabilities. Based on the results of the forensic investigation, on December 20, 2024, GBP discovered that the malicious code may have allowed an unauthorized third party to view or acquire certain customer information entered at the checkout that used a limited set of payment options on the Pro Shop website between September 23-24, 2024 and October 3-23, 2024, including 47 Maryland residents. Purchases on the Pro Shop website that were made using a gift card, Pro Shop website account, Paypal, or Amazon Pay, were not affected by this malicious code.

The information that may have been accessed or acquired included certain information entered on the Pro Shop website when making a purchase, and may have included customers' name, address (billing and shipping), email address, credit card type, credit card number, credit card expiration date, and credit card verification number. As noted above, if customers made purchases on the Pro Shop website using a gift card, Pro Shop website account, Paypal, or Amazon Pay, their information was not affected by this malicious code. Affected individuals will receive written notification of this incident sent via U.S. Mail postmarked on or around January 6, 2025. A copy of the template notice to individuals is attached.

GBP is offering affected individuals complimentary access to 36 months of credit monitoring and identity theft restoration services through Experian. GBP is also notifying the three largest nationwide consumer reporting agencies, including Equifax, Experian and TransUnion, of this incident.

GBP took immediate action to investigate once we learned of the potential incident. GBP's IT team, in conjunction with outside cybersecurity experts and the vendor that hosts the Pro Shop website, worked to successfully contain and remediate the security incident. Since that time, GBP has continued to take a number of steps to enhance GBP's security protocols and controls, technology, and training. GBP also worked with the vendors that host and manage the Pro Shop website to confirm enhancements to their security protocols. GBP continues to assess further options to protect its systems.

For further information and assistance, please contact me, GBP's outside legal counsel, at 414-277-5423 or Meghan.OConnor@quarles.com.

Sincerely yours,

QUARLES & BRADY LLP



Meghan C. O'Connor

Attachment

Green Bay Packers, Inc.
Return Mail Processing
PO Box 999
Suwanee, GA 30024

1 1 1 *****AUTO**MIXED AADC 302

SAMPLE A. SAMPLE - L01

APT ABC

123 ANY ST

ANYTOWN, US 12345-6789



January 6, 2025

NOTICE OF DATA BREACH

Dear Sample A. Sample,

The Green Bay Packers, Inc. (“we” or “our”) are writing to inform you of a data security incident that occurred on the website, packersproshop.com (“Pro Shop website”), that may have affected your personal information. Below are details of what happened, the steps we are taking to resolve the situation, and what we are doing to support potentially affected individuals.

WHAT HAPPENED?

On October 23, 2024, we were alerted to the presence of malicious code inserted on the Pro Shop website by a third party threat actor. Immediately upon learning this, we temporarily disabled all payment and checkout capabilities on the Pro Shop website and began an investigation. We engaged outside cybersecurity experts to assist with this investigation and determine what, if any, customer information may have been affected. We also immediately required the vendor that hosts and manages the Pro Shop website to remove the malicious code from the checkout page, refresh its passwords, and confirm there were no remaining vulnerabilities. Based on the results of the forensic investigation, on December 20, 2024 we discovered that the malicious code may have allowed an unauthorized third party to view or acquire certain customer information entered at the checkout that used a limited set of payment options on the Pro Shop website between September 23-24, 2024 and October 3-23, 2024. **Purchases on the Pro Shop website that were made using a gift card, Pro Shop website account, Paypal, or Amazon Pay, were not affected by this malicious code.**

WHAT INFORMATION WAS INVOLVED?

The information that may have been accessed or acquired included certain information entered on the Pro Shop website when making a purchase, and may have included your name, address (billing and shipping), email address, credit card type, credit card number, credit card expiration date, and credit card verification number. **As noted above, if you made purchases on the Pro Shop website using a gift card, Pro Shop website account, Paypal, or Amazon Pay, your information was not affected by this malicious code.**

WHAT ARE WE DOING?

We took immediate action to investigate once we learned of the potential incident. Our IT team, in conjunction with outside cybersecurity experts and the vendor that hosts the Pro Shop website, worked to successfully contain and remediate the security incident. Since that time, we have continued to take a number of steps to enhance our security protocols and controls, technology, and training. We also worked with our vendors that host and manage the Pro Shop website to confirm enhancements to their security protocols. We continue to assess further options to protect our systems.

We are offering you complimentary access to 36 months of credit monitoring and identity theft restoration services through Experian. If you wish to take advantage of this access, you will need to enroll yourself in these services, as we are not able to activate them on your behalf. Please review the instructions in the attached *Information on Credit Monitoring & Identity Theft*.

Green Bay Packers, Inc. • 1265 Lombardi Ave., Green Bay, WI 54304 • 920-569-7500

WHAT CAN YOU DO?

In addition to enrolling in credit monitoring, we always recommend that you follow best practices and remain vigilant for incidents of fraud and identity theft as described below. You can review your account statements and monitor free credit reports (in addition to the complementary credit monitoring and identity theft restoration services). Promptly report any fraudulent activity or any suspected incidents of identity theft to your bank or other financial institution holding your accounts, as well as any appropriate authorities, such as your state attorney general and the Federal Trade Commission (“FTC”). Individuals also have the right to obtain a police report in the event one has been created for this incident.

FOR MORE INFORMATION

For more information and assistance, please contact 833-931-4653, Monday through Friday from 8:00am to 8:00pm Central Time (excluding major US holidays).

Please know that we take this matter very seriously, and we apologize for any stress or concern this may cause.

Sincerely,

A handwritten signature in cursive script that reads "C/ Jorgensen".

Chrysta Jorgensen
Director of Retail Operations
Green Bay Packers, Inc.

INFORMATION ON CREDIT MONITORING & IDENTITY THEFT

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for 36 months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for 36 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 36-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by April 30, 2025** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bcredit>
- Provide your **activation code**: ABCDEFGHI

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 833-931-4653 by April 30, 2025 (5:59 UTC). Be prepared to provide engagement number B137437 as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 36-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARETM:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance^{**}:** Provides coverage for certain costs and unauthorized electronic fund transfers.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.



Individuals are advised to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports and to promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general as well as the Federal Trade Commission.

The following are some resources:

Federal Trade Commission ("FTC")

www.ftc.gov/idtheft

1-877-ID-THEFT (1-877-438-4338)

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Take Charge: Fighting Back Against Identity Theft

This is a comprehensive guide from FTC to help guard against and deal with identity theft <https://www.identitytheft.gov/>.

Credit Bureaus

You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting www.annualcreditreport.com, calling 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at www.annualcreditreport.com/manualRequestForm.action

Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is as follows:

Equifax 1-800-685-1111 www.equifax.com/personal/credit-report-services/ P.O. Box 740241 Atlanta, GA 30374	Experian 1-888-397-3742 www.experian.com P.O. Box 4500 Allen, TX 75013	TransUnion 1-800-888-4213 www.transunion.com/fraud P.O. Box 1000 Chester, PA 19016
--	---	---

You can obtain additional information from the FTC and the nationwide credit reporting agencies about placing a security freeze on your credit files and fraud alerts. A security freeze is a free tool that lets you restrict access to your credit report, which in turn makes it more difficult for identity thieves to open new accounts in your name. To place a security freeze on your credit files, contact each of the nationwide credit bureaus using the contact information listed above. You will need to supply your name, address, date of birth, social security number, and other personal information. You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies using the contact information listed above.

FOR MARYLAND RESIDENTS

You can obtain information about preventing identify theft from the FTC or:

Maryland Attorney General:

Visit the Maryland Office of the Attorney General, Identity Theft Unit at:

<http://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx>

or call 410-576-6491

or write to this address:

Maryland Office of the Attorney General
Identity Theft Unit
16th Floor
200 St. Paul Place
Baltimore, MD 21202

FOR NEW MEXICO RESIDENTS

You have rights pursuant to the Fair Credit Reporting Act. We encourage you to review these rights by visiting https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or by writing to Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

FOR NEW YORK RESIDENTS

You can obtain information about preventing identity theft from:
New York Department of State Division of Consumer Protection: www.dos.ny.gov/consumer-protection
NYS Attorney General at: www.ag.ny.gov

FOR NORTH CAROLINA RESIDENTS

You can obtain information about preventing identify theft from the FTC or:

North Carolina Attorney General:

Visit the North Carolina Office of the Attorney General at:

www.ncdoj.gov or call 1-877-566-7226

or write to this address:

Attorney General's Office

9001 Mail Service Center

Raleigh, NC 27699-9001

FOR RHODE ISLAND RESIDENTS

6 individuals in Rhode Island were affected by this incident. You can obtain information about preventing identity theft from:

Rhode Island Attorney General:

Visit the Rhode Island Office of the Attorney General at:

www.riag.ri.gov, or call (401) 274-4400

or write to this address:

Rhode Island Office of the Attorney General

Consumer Protection Unit

150 South Main Street

Providence, RI 02903

FOR WASHINGTON D.C. RESIDENTS

You may obtain information about preventing identify theft from the FTC or the following:

Washington D.C. Attorney General:

Visit the Washington Office of the Attorney General (OAG) at:

<https://oag.dc.gov/>, or call the OAG's Office of Consumer Protection at 202-442-9828

or write to this address:

Office of the Attorney General

400 6th Street, NW

Washington, DC 20001

